УДК 681.3.06

В.И. Долгов

Харьковский национальный университет радиоэлектроники

ЭЛЛИПТИЧЕСКИЕ КРИВЫЕ В КРИПТОГРАФИИ

Определяются условия, которые должны быть учтены при отборе эллиптических кривых для криптографических применений. Приводится соответствующий понятийный аппарат, в частности определяются понятия сингулярности и суперсингулярности для эллиптических кривых и рассматриваются теоретические положения, лежащие в их основе.

Ключевые слова: *криптография, эллиптическая кривая, сингулярность, суперсингулярность.*

Введение

Заинтересованность математическими конструкциями в виде группы рациональных точек эллиптических кривых возникла в криптографии в 1985 г. в двух направлениях: для решения задач факторизации больших целых чисел и для построения криптографических протоколов [1, 2]. Эта заинтересованность особенно актуализировалась в последние десятилетия и обусловлена она тем, что с одной стороны, эллиптические кривые оказались источником конечных абелевых групп, которые владеют полезными структурными свойствами, а с другой – тем, что на основе их применения удалось обеспечить те же показатели стойкости, которыми владеют числовые и полиномиальные криптосистемы, но соответствующие показатели первых удалось получить при существенно меньшем размере ключа. Многие трудности, связанные со сложной математикой и реализационными особенностями за прошедшие годы были успешно преодолены, и сегодня уже можно говорить о действующих стандартах цифровой подписи, в том числе и украинском стандарте ДСТУ4145-2002, которые строятся с использованием арифметики эллиптических кривых над конечными полями.

Широкое внедрение в практику проектирования и разработки систем криптографической защиты информации технологий с использованием эллиптических кривых стимулировали включение в учебные программы Ввузов, ведущих подготовку специалистов соответствующего профиля, новых разделов математики и дополнительных разделов в специальные дисциплины, обеспечивающих освоение нового направления развития криптологии. Объем дополнительных учебных вопросов, и повышенный уровень их сложности здесь входит в противоречие с имеющимся бюджетом учебного времени. Приходится мириться с порой недостаточно глубоким изложением многих принципиальных положений в надежде, что желающие могут почерпнуть дополнительную более содержательную информацию из рекомендуемой литературы в часы самостоятельной работы.

В настоящей публикации излагается ряд вопросов общетеоретического характера, определяющих условия и возможности применения эллиптических кривых для построения протоколов и алгоритмов криптографической защиты информации, с целью облегчить освоение нового и далеко не простого понятийного аппарата и ориентацию в большом потоке публикаций, посвященных рассматриваемому направлению.

Безусловно, что одним из основных показателей криптоалгоритмов выступает уровень их стойкости. Как показывает анализ, не все эллиптические кривые в оговоренном смысле одинаково полезны и пригодны для использования. В этой работе мы определим условия, которые должны быть учтены при отборе эллиптических кривых пригодных для криптографических применений.

1. Условие несингулярности кривой

Итак, наше внимание сосредотачивается на *эллиптических кривых* E, которые задаются уравнением в канонической *форме Вейерштрасса*

$$E: y^2 = x^3 + ax^2 + bx + c. \qquad (1)$$

Кубическое уравнение общего вида представляют также и в таком виде

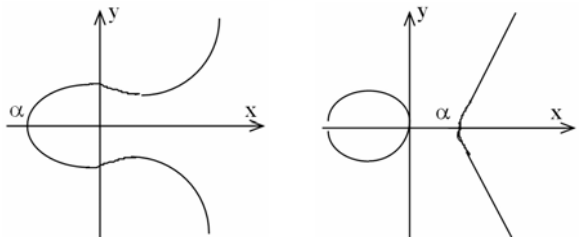
$$y^2 = f(x),\ f(x) = x^3 + ax^2 + bx + c, \qquad (2)$$

т.е. правая часть равенства рассматривается как обычный многочлен третьей степени.

В дальнейшем, будем считать коэффициенты a, b, c функции $f(x)$ рациональными, в частности, действительными числами, и, значит, многочлен $f(x)$ степени 3 имеет, по меньшей мере, один действительный корень. В действительных числах мы можем разложить его на множители как

$$f(x) = (x - \alpha)(x^2 + \beta x + \gamma),$$

где α, β, γ – действительные числа. Если многочлен имеет один действительный корень, то кривая имеет вид, подобный рис. 1, а, так как $y = 0$, когда $x = \alpha$. Если $f(x)$ имеет все три действительных корня, то кривая имеет вид, подобный показанному на рис. 1, б. В этом случае действительные точки образуют две компоненты. Последнее справедливо при условии, что корни уравнения $f(x) = 0$ разные. Именно этот случай нас и будет интересовать. Что существенно для этого условия?



а б

Рис. 1. Вид эллиптической кривой E для полинома: а – с одним корнем, б – с тремя корнями

Напомним, что эллиптическую кривую мы будем использовать для образования группы с ее точек. Как известно [3, 4], операция в группе точек эллиптической кривой связана с геометрическими построениями (*для любых точек* P *и* Q *точка* $P * Q$ – *это третья точка пересечения прямой* $g = \overline{PQ}$ *с кривой* E*, симметрично отраженная относительно оси Ox*). Поэтому нас, прежде всего, должны интересовать условия существования соответствующих геометрических элементов (хорд и касательных) для произвольных точек кривой.

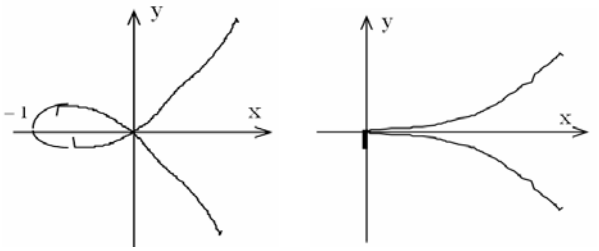
Запишем уравнение кривой в виде $F(x, y) = y^2 - f(x) = 0$ и возьмем частные производные $\frac{\partial F}{\partial x} = -f'(x)$, $\frac{\partial F}{\partial y} = 2y$. Если частные производные стремятся в некоторой точке (x_0, y_0) кривой к нулю, то $y_0 = 0$ и, следовательно, многочлены $f(x)$ и $f'(x)$ имеют общий корень x_0, т.е. x_0 является двойным корнем функции $f'(x)$, и наоборот, если f имеет двойной корень x_0, то $(x_0, 0)$ будет так называемой *сингулярной* точкой на кривой. По определению под сингулярной понимают точку, в которой производная равняется нулю или не существует. Если эллиптическая кривая имеет сингулярную точку, то и самая кривая называется *сингулярной*. Соответственно мы будем иметь *несингулярную кривую* при условии, что не существует точки на кривой, в которой частные производные одновременно исчезают. Это и будет означать, что каждая точка на кривой имеет полностью определенную касательную.

Покажем теперь более строго, что мы действительно должны сфокусироваться именно только на несингулярных кубах? Это сразу не так понятно. Следуя [3] рассмотрим сингулярный случай более подробно. Возможны две картины сингулярности. Какая из них возникает, зависит от того, имеет ли f(x) двойной корень или тройной. В случае, если такая функция имеет двойной корень, типичным будет уравнение

$$y^2 = x^2(x+1),$$

и кривая имеет сингулярную точку с разными направлениями касательных, как показано на рис. 2, а, т.е. касательная в этой точке определяется неоднозначно.

Если f(x) имеет тройной корень, то уравнение может быть преобразовано к виду $y^2 = x^3$. Это полукубическая парабола с вершиной в начале координат. Если $f'(x)$ имеет тройной корень, то уравнение может быть преобразовано к виду $y^2 = x^3$. Это полукубическая парабола с вершиной в начале координат (рис. 2, б). Существуют и другие примеры сингулярных кубов в форме Вейерштрасса, но они также приводятся к общему виду после изменения координат.



а б

Рис. 2. Две картины сингулярности

Дело в том, что рациональным точкам на сингулярном кубе могут быть поставлены во взаимно однозначное соответствие рациональные точки на прямой (если мы спроецируем сингулярную точку на некоторую прямую, то мы увидим, что прямая, которая проходит через сингулярную точку, пересекает куб дважды, и значит она пересекает куб еще только один раз). Таким образом, проекция кубической кривой на прямую является взаимно однозначным отображением.

Фактически это легко сделать явным образом с помощью формулы. Действительно, если мы примем $r = y / x$, то уравнение $y^2 = x^2(x+1)$ превращается в $r^2 = x + 1$ и значит $x = r^2 - 1$ и $y = r^3 - r$. Для каждого рационального числа r можно определить x и y, т.е. получить рациональную точку на кубе; а если мы начнем из рациональной точки (x, y) на кубе, то мы получим рациональное число r. Эти операции являются инверсными одна другой и определяются для всех рациональных точек, кроме сингулярной точки $(0, 0)$ на кривой. Но тогда это означает, что таким способом мы можем получить все рациональные точки на кривой.

Кривая $y^2 = x^3$ еще проще. Мы только примем $x = t^2$ и $y = t^3$.

Таким образом, в случае сингулярной кривой мы приходим к тому, что вместо множества ее рациональных точек можно рассматривать множество точек некоторой прямой (за счет существования отмеченного взаимно однозначного соответствия между ними). Итак, *сингулярные кубы являются тривиальными для анализа*, как и рациональные точки на них. Группу, однако, можно получить, если избегать сингулярности[1]. Итак, в дальнейшем нас будут интересовать несингулярные эллиптические кривые, т.е. кривые, что не имеют точек, в которых

[1] Рациональные точки на сингулярных и несингулярных кубических кривых ведут себя совсем по- разному: группа рациональных точек на сингулярной кривой не является конечно порожденной, в той время как группа рациональных точек на несингулярной кривой – конечно порожденная.

производные $\frac{\partial F}{\partial x} = -f'(x)$, $\frac{\partial F}{\partial y} = 2y$ одновременно исчезают (равняют нулю). Такие кривые называют также *гладкими*.

Полезно отметить, что с гладкостью кривой часто связывают понятие *дискриминанта* D(f). Это понятие появляется при изучении алгебраических уравнений. Дискриминантом D(f) алгебраического уравнения $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 = 0$, $a_n \neq 0$ является произведение a_n^{2n-2} и квадратов всех разностей $x_i - x_k$ $(i > k)$ корней x_i уравнения (кратные корни порядка *m* рассматриваются как *m* разных корней с разными индексами):

$$D(f) = a_n^{2n-2}\prod_{i>k}(x_i - x_k)^2 = a_n^{2n-2}\left[W(x_1, x_2, \ldots, x_n)\right]^2,$$

где определитель Вандермонда $W(x_1, x_2, \ldots, x_n) =$

$$= \begin{vmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \cdots & x_2^{n-1} \\ \cdot & \cdot & \cdot & \cdots & \cdot \\ 1 & x_n & x_n^2 & \cdots & x_1^{n-1} \end{vmatrix} = \prod_{i>k}(x_i - x_k) /$$

Дискриминант D(f) является симметрической[2] функцией корней $x_1, x_2, \ldots, x_n$, которая обращается в нуль в том и только в том случае, когда $f(x)$ имеет, по меньшей мере, один кратный корень (который необходимо оказывается корнем $f(x)$ и $f'(x)$).

Вычислим, например, дискриминант кубического трёхчлена $f(x) = x^3 + bx + c$, корнями которого являются α_1, α_2, α_3. Пользуясь приведенной выше формулой, получаем

$$D(f) = (-1)^{3\cdot 2/2} f'(\alpha_1)f'(\alpha_2)f'(\alpha_3) =$$

$$= -(3\alpha_1^2 + b)(3\alpha_2^2 + b)(3\alpha_3^2 + b) = -\Big[27\alpha_1^2\alpha_2^2\alpha_3^2 +$$

$$+ 9p(\alpha_1^2\alpha_2^2 + \alpha_1^2\alpha_3^2 + \alpha_2^2\alpha_3^2) + 3b^2(\alpha_1^2 + \alpha_2^2 + \alpha_3^2) + b^3\Big].$$

Поскольку $\alpha_1^2\alpha_2^2 + \alpha_1^2\alpha_3^2 + \alpha_2^2\alpha_3^2 =$

$$= (\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3)^2 - 2\alpha_1\alpha_2\alpha_3(\alpha_1 + \alpha_2 + \alpha_3);$$

$$\alpha_1^2 + \alpha_2^2 + \alpha_3^2 = (\alpha_1 + \alpha_2 + \alpha_3) - 2(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3),$$

и, кроме того, $\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 = b$, $\alpha_1\alpha_2\alpha_3 = -c$, $\alpha_1 + \alpha_2 + \alpha_3 = 0$ то $D(f) = -4b^3 - 27c^2$.

Для кривой в нормальной форме (2) дискриминантом функции $f(x)$ является величина

$$D(f) = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2.$$

Более знакомой является форма $D(f) = -4b^3 - 27c^2$, которая отвечает случаю $a = 0$ в уравнении (1) (см. пример, приведенный выше). В соответствии с известным определением и теоремой [5] (*многочлен* $f(x)$ *имеет кратный корень тогда и только тогда, когда его дискриминант равняется нулю*), если дискриминант не оборачивается в нуль, то это говорит о том, что корни $f(x)$ являются разными. Таким образом, *эллиптическая кривая с рациональными коэффициентами* (*т.е. над полем* **R**) *с ненулевым дискриминантом* $D(f) \neq 0$ *представляет собой гладкую кривую, в каждой точке которой можно провести касательную*.

2. Спаривание Вейля и дискретный логарифм

Обсуждая условия отбора эллиптических кривых для криптографических применений, надо подчеркнуть, что сегодня криптография на эллиптических кривых уже вышла на уровень принятия стандартов, т.е. выполненные исследования и разработки уже разрешили перейти к практической реализации алгоритмов преобразований в группах точек эллиптических кривых. В процессе выполнения исследований обнаружилось дополнительное ограничение к выбору эллиптических кривых, связанное с понятием *суперсингулярности*, на котором мы сейчас сосредоточим внимание.

Для дальнейшего понимания нужно будет сначала кратко изложить некоторые принципы построения криптографических алгоритмов и обеспечения их стойкости. Начнем с того, что одним из мощных криптографических инструментов являются так называемые *труднообратимые* (*однопутевые*) *функции*. Общая концепция построения однопутевых функций состоит в конструировании большой конечной циклической группы $\mathbf{G} = \langle G; \circ \rangle$ вместе с порождающим элементом (генератором) $g \in G$ таким, чтобы было "легко" вычислить кратное $m \cdot g := g \circ \ldots \circ g$ для всех $m \in N$, но чтобы было "тяжело" восстановить *m* для некоторого произвольного элемента $h \in G$ такого, что $m \cdot g = h$. Здесь "легкое" вычисление означает, что оно может быть выполнено за полиномиальное время, где полином имеет степень порядка $\log|G|$, а "трудное" вычисление означает сложность намного большую чем полиномиальная, по крайней мере, для лучшего из известных алгоритмов. Одной из реализаций этой конструкции является возведение в степень (экспоненцирование) в большом конечном поле, которое предложено Диффи и Хеллманом [7]. Этот принцип используется, в частности, для построения криптосистем с публичными (открытыми) ключами[3] и на эллиптических кривых.

В криптографических применениях эллиптическая кривая рассматривается над конечным полем

[2] Симметрическая функция – функция, которая не меняется при любой перестановке своих аргументов.

[3] В криптосистемах с публичными (открытыми) ключами используются параметры шифров, которые являются общедоступными (известными) для всех пользователей системы (в данном случае открытыми параметрами являются координаты точки $P = (x, y)$).

$GF(q)$, т.е. кубическая кривая *E* определяется как множество всех точек $(x, y) \in GF(q) \times GF(q)$, которые удовлетворяют уравнению (1) с коэффициентами $a, b, c \in GF(q)$. Для выполнения криптопреобразований используются точки $P \in E(GF(q))$ [4] эллиптических кривых *E* над конечными полями $GF(q)$, которые образуют группу относительно операции сложения точек [4]. Трудно обратимое преобразование в этом случае заключается в вычислении точки, которая является кратной некоторому порождающему элементу группы точек эллиптической кривой. Оно имеет именно такой вид, о котором мы говорили выше:

$$Q = kP,\ Q \in \langle P \rangle.$$

Здесь P называется базовой точкой эллиптической кривой[5] (ее называют также генератором), k – некоторое целое число, $1 < k < n$. Эта базовая точка должна иметь большой порядок. Тогда сравнительно легко вычислить скалярное произведение kP ($kP = P + P + \ldots + P$ k-раз), но трудно вычислить k по известным значением Q и P. Задача определения множителя k по известным значением Q и P получила название дискретного логарифмирования.

Сущность задачи дискретного логарифмирования в данном случае заключается именно в том, чтобы по известным значением Q и P найти множитель k (если операцию трактовать как умножение, то очевидное соответствие между аддитивной и мультипликативной группами $P + P + \ldots + P = kP \to P \circ P \circ \ldots \circ P = P^k$, что и оправдывает использование понятия логарифмирования в случае аддитивной группы). Стойкость этого криптографического преобразования определяется сложностью решения задачи дискретного логарифмирования в циклической группе $\langle P \rangle$ большого простого порядка n; в нашем случае порядка группы точек эллиптической кривой E, порожденной базовой точкой этой кривой P.

Теперь можно возвратиться к очередному ограничению к выбору эллиптических кривых. Напомним сначала, что еще в 1987 году Коблиц [8] предложил для криптосистем с открытыми ключами использовать так называемые суперсингулярные кривые с конечным числом $\#E(GF(q)) = q + 1$ элементов (точек на кривой). Однако позднее было показано, что такие кривые не пригодны для криптографических применений. Криптосистемы, которые базируются на кривых такого типа, могут быть атакованы алгоритмом дискретного логарифмирования, предложенным еще в 1993 г. А. Менезисом, Т. Окомото и С. Венстоном [9]. Этот алгоритм использует так называемое спаривание Вейля для приведения группы точек эллиптической кривой над полем $GF(2^m)$ к мультипликативной группе некоторого расширения $GF(2^{lm})$ исходного конечного поля, которое позволяет свести проблему дискретного логарифмирования на кривой к проблеме дискретного логарифмирования в конечном поле. Позднее были приложены усилия заменить эллиптические кривые, предложенные Коблицем, некоторыми другими суперсингулярными кривыми, которые ожидались более надежными для применения. Однако, и эти кривые допускали приведения к некоторому конечному полю большого размера.

Итак, коротко напомним сущность алгоритма приведения, предложенного А. Менезисом, Т. Окомото и С. Венстоном[6]. Как уже было указано, главная идея подхода состоит в том, чтобы привести вычисление дискретного логарифма в группе точек эллиптической кривой E(K), которая рассматривается над полем K, к проблеме дискретного логарифмирования в конечном поле GF, путем сведения группы точек E(K) к мультипликативной группе конечного поля GF.

Нам будут нужны несколько новых фактов из теории эллиптических кривых. Мы уже договорились, что точки эллиптической кривой с введенной на множестве точек операцией сложения (умножения) точек вместе с точкой на бесконечности O образуют группу [3, 4]. Очевидно дальше, что любая точка P конечного порядка n образует подгруппу $E[n]$ группы точек эллиптической кривой. Такая подгруппа называется *группой кручения*[7] эллиптической кривой. Если n – нечетное число, то порядок группы кручения равняется n^2 ($P = (x_p, y_p) \in K \times K$). Криптографические алгоритмы строятся именно в циклической группе простого порядка n. Эта циклическая группа является подгруппой группы кручения. Остальные точки группы кручения не принадлежат основному полю (подполю из n элементов). Поскольку группа кручения конечная, то существует расширение $GF(2^{ml})$ исходного поля[8], в котором лежат все точки группы кручения. Мультипликативная группа этого расширения имеет порядок $2^{ml} - 1$, поэтому соответственно теореме Лагранжа [5] вложение группы кручения в мультипликативную группу этого расширения возможно только в том случае, если n делит $2^{ml} - 1$. Оказалось, что этого условия и достаточно. Указанный факт и лежит в основе метода сведения задачи дискретного логарифмирования в группе точек эллиптической кривой к задаче дискретного ло-

[4] E(GF(q)) – обозначение эллиптической кривой *E* над полем GF(q).

[5] Символом (P) обозначена циклическая группа, порожденная элементом P (см. [4]).

[6] Сейчас уже предложен и ряд других алгоритмов приведения (спаривания Frey – Ruck (1994), Mstsunari-Sakai-Kasahara (1999) и др.).

[7] Кручение конечно порожденной абелевой группы G – группа T, которая состоит из всех элементов конечного порядка ν группы G. Числа $\nu > 1$ могут быть однозначно с точностью до перестановки выбраны в виде степеней простых чисел, и тогда они называются коэффициентами кручения группы G.

[8] Тут речь идет о расширении двоичного поля.

гарифмирования в мультипликативной группе расширения исходного конечного поля, для которой, существуют алгоритмы решения задачи дискретного логарифмирования субэкспоненциальной сложности. Фактически это сведение выполняется с помощью так называемого спаривания Вейля, которое является отображением вида

$$e_N : E[n] \times E[n] \to \mu_n ,$$

где μ_n – группа корней степени n из единицы, которая при приведенном условии является подгруппой мультипликативной группы конечного поля $GF(2^{lm})$. Если $Q = kP$ и T – точка из $E[n]$, которая не принадлежит $\langle P \rangle$, то для $e_N(P, T) = \alpha \in \mu_n$ и $e_N(Q, T) = \beta \in \mu_n$ при условии, что отображение e_N есть билинейным[9] и невырожденным[10], выходит $\beta = \alpha^k$. Этот и означает, что задача дискретного логарифмирования выражения $Q = kP$ в циклической группе $\langle P \rangle$ сводится к задаче дискретного логарифмирования $\beta = \alpha^k$ в конечном поле $GF(2^{lm})$.

Если степень расширения l мала, то для исходной задачи дискретного логарифмирования существует субэкспоненциальный алгоритм. Например, в случае очень интересных с вычислительной точки зрения суперсингулярных кривых вышло так, что $l \le 6$, поэтому при относительно малых размерах основного поля пришлось отказаться от применения таких кривых в криптографии.

Таким образом, мы пришли еще к одному условию отбора кривых для использования в криптографии, которое получило название MOV (условие Менезиса-Окомото-Венстона): порядок базовых точек эллиптических кривых, которые разрешаются к криптографическому использованию, должен удовлетворять ограничению $2^{ml} \neq 1 (\mathrm{mod}\, n)$, для $1 \le l \le 32$.

Это означает, что циклическая группа, которая порождается базовой точкой, должна иметь большой порядок (соображение, приведенные выше касаются расширений полей характеристики 2, т.е. в общем случае речь должна идти о конечном расширении $GF(p^k)$.

Заметим здесь, что дискретный логарифм в конечном поле $GF(2^n)$ может быть вычислен с помощью алгоритма Копершмита [10] со сложностью

$$O(\exp(cn^{1/3}(\ln n)^{2/3}) .$$

В дальнейшем оказалось, что MOV условие может быть выполнено, если воспользоваться несуперсингулярными эллиптическими кривыми.

Итак, остановимся на понятиях суперсингулярности и несуперсингулярности, а также на условиях выполнения требования несуперсингулярности более подробно.

[9] Билинейность спаривания $e_N([n]P, Q) = e_N(P, [n]Q) = e_N(P, Q)^n$.

[10] Невырожденность спаривания $e_N(P, P) \neq 1$.

3. Условия несуперсингулярности кривой

Сосредоточим внимание на теоретическом обосновании MOV условия и связанных с ним некоторых новых понятиях и определениях (суперсингулярности, билинейности отображения, и т.д.), которые появились при изложении спаривания Вейля. Нам для этого придется познакомиться с дополнительными более сложными обобщениями и построениями из теории полей Галуа. Начнем с обсуждения важных следствий, которые вытекают из теоремы Мордела[11]. Напомним, что в соответствии с теоремой Мордела *группа* $C(\mathbf{Q})$ *рациональных точек на несингулярной кривой* (1) *является конечно порожденной абелевой группой*, а из фундаментальной теореме по абелевым группам [4]: *всякая конечно порожденная абелева группа раскладывается в прямую сумму конечного числа неразложимых циклических подгрупп, из которых часть – конечно примарные*[12]*, часть – бесконечные*) вытекает, что $C(\mathbf{Q})$, как абстрактная группа, изоморфна прямой сумме бесконечных циклических групп, и конечных циклических групп простого порядка.

Следуя работе [3], объясним этот момент более подробно. Пусть $\mathbf{Z}$ обозначает аддитивную группу целых чисел, и пусть Z_m обозначает циклическую группу $\mathbf{Z}/m\mathbf{Z}$ целых чисел по модулю m (факторкольцо целых чисел по модулю m). Тогда структурная теорема говорит нам о том, что группа $C(\mathbf{Q})$ имеет вид подобный такому

$$C(\mathbf{Q}) \cong \underbrace{\mathbf{Z} \oplus \mathbf{Z} \oplus \cdots \oplus \mathbf{Z}}_{r\ p \in K\mu\%o} \oplus \mathbf{Z}_{p_1}^{\nu_1} \oplus \mathbf{Z}_{p_2}^{\nu_2} \oplus \cdots \oplus \mathbf{Z}_{p_s}^{\nu_s} . \quad (3)$$

Если говорить проще, приведенная запись свидетельствует, что существуют генераторы (порождающие элементы)

$$P_1, \ldots, P_r, Q_1, \ldots, Q_s \in C(\mathbf{Q}) ,$$

которые позволяют каждую точку $P \in C(\mathbf{Q})$ эллиптической кривой записать в виде

$$P = n_1P_1 + \ldots + n_rP_r + m_1Q_1 + \ldots + m_sQ_s .$$

Здесь целые числа n_i уникально определены точкой P, в то время как целые числа m_j определяются по соответствующим модулям $p_j^{\nu_j}$, j = 1, 2, ... , s. Целое число r называется рангом группы $C(\mathbf{Q})$. Группа C(Q) может быть конечной, если и только если она

[11] Еще в 1901 году французский математик А. Пуанкаре высказал гипотезу о том, что *всегда можно найти такое конечное число рациональных точек* $P_1, P_2, \ldots, P_r$ *бесконечного порядка, что любая рациональная точка P выражается через них, т.е. представляется в виде* $P = P_1n_1 + P_2n_2 + \ldots P_rn_r + Q$, *где* $n_1, n_2, \ldots n_r$ – *целые числа, которые определяются однозначно точкой* P, *а* Q – *точка конечного порядка. Сами же точки* $P_1, P_2, \ldots n_r$ *не выражаются одна через другие.* Именно эту гипотезу в 1922 году доказал английский математик Л. Морделл

[12] Примарная группа – периодическая абелева группа, порядки всех элементов которой являются степенью фиксированного простого числа *p* [4].

имеет ранг $r = 0$. Подгруппа $\mathbf{Z}_{p_1}^{v_1} \oplus \mathbf{Z}_{p_2}^{v_2} \oplus \cdots \oplus \mathbf{Z}_{p_s}^{v_s}$ соответсвует элементам конечного порядка в C(Q); она имеет порядок $p_1^{v_1} \cdot p_2^{v_2} \cdots p_s^{v_s}$.

Обычно точки $P_1, ..., P_r, Q_1, ..., Q_s$ не являются уникальными. Существует много возможных вариантов генераторов для C(Q).

Мы пока что говорили о рациональных точках, но фактически уравнение кубической кривой (1) определяет несколько множеств точек. Мы можем записать C(**Q**) для множества точек кривой, чьи координаты оказываются рациональными, C(**R**) для точек, которые имеют действительные координаты и C(**C**) для множества пар комплексных чисел (x, y), что удовлетворяют уравнению (1). Существует также точка O на бесконечности, которую мы считаем присутствующей во всех таких множествах.

Пользуясь законом сложения, легко убедить, что точки кривой с комплексными координатами тоже образуют группу. Точки с действительными координатами образуют подгруппу этой группы. А потому что мы допускаем, что коэффициенты уравнения кривой a, b, c являются рациональными числами, то верно и то, что ее рациональные точки образуют подгруппу группы действительных чисел. Итак, мы имеем группу и несколько подгрупп:

$$\{O\} \subset C(\mathbf{Q}) \subset C(\mathbf{R}) \subset C(\mathbf{C}).$$

В конечном итоге нас будут интересовать точки эллиптических кривых, координаты которых рассматриваются как элементы полей, и их расширений. Поэтому для дальнейшего полезно будет напомнить некоторые факты, которые касаются общей теории расширений полей и теории Галуа. Итак, рассмотрим поле комплексных чисел со своими подполями $\mathbf{Q} \subset K \subset \mathbf{C}$. В данном случае поле K, как расширение поля **Q**, является **Q**-векторным пространством, со *степенью расширения* K *над* **Q**, которая является размерностью линейного пространства [4]: *каждое расширение* Ω *можно рассматривать как линейное пространство над полем* Δ. Напомним также, что степень расширения поля K над **Q** обозначается как $|\Omega: \Delta|$).

Если степень расширения $|K : \mathbf{Q}|$ конечная [4]: *степень конечного расширения* Ω *над полем* Δ *равняется максимальному числу элементов поля* Ω*, которые в состоянии образовать линейно независимую систему*), то мы будем говорить, что K является *числовым полем.*

Важным методом изучения числовых полей является рассмотрение множества полевых гомоморфизмов

$$\sigma: K \to \mathbf{C}.$$

Подчеркнем, что гомоморфизм полей всегда является взаимно однозначным отображением (изоморфизмом), так как поле не имеет нетривиальных идеалов. Заметим также, что по свойствам гомоморфизмов колец $\sigma(1) = 1$ [4], и обратный элемент переходит в обратный, т.е. $\sigma(a^{-1}) = \sigma(a)^{-1}$, и потому всякий гомоморфизм полей σ автоматически будет удовлетворять условию $\sigma(a) = a$ для всех $a \in \mathbf{Q}$. Это свидетельствует о том, что число гомоморфизмов $K \to \mathbf{C}$ всегда точно будет равнять степени расширения $|K : \mathbf{Q}|$ (гомоморфизм полей – это всегда вложение).

Иногда случается так, что образ $\sigma(K)$ равняется исходному полю K. Тогда σ действительно является гомоморфизмом K на самого себя, и в таком случае мы будем называть σ *автоморфизмом* поля K. Заметим, однако, что это не означает равенства $\sigma(\alpha) = \alpha$ для каждого $\alpha \in K$, а просто означает, что $\sigma(\alpha) \in K$. Если это случается для каждого отображения σ, то K называется *Галуа расширением* **Q** [3]. Более обобщенно, определим

$$\mathrm{Aut}(K) = \{\text{автоморфизмы } \sigma : K \to K\}.$$

Очевидно, что Aut(*K*) является группой, так как если $\sigma, \tau \in \mathrm{Aut}(K)$, то тогда мы можем сформировать элемент $\sigma\tau \in \mathrm{Aut}(K)$, путем определения композиции $(\sigma\tau)\,\alpha = \sigma(\tau(\alpha))$. Числовое поле K является Галуа расширением **Q**, если и только если

$$\#\mathrm{Aut}(K) = |K : \mathbf{Q}|.$$

В этом случае будем записывать $\mathrm{Gal}(K/\mathbf{Q})$ вместо Aut(K) и называть $\mathrm{Gal}(K/\mathbf{Q})$ *группой Галуа*[13] K/**Q**. Нас здесь будет интересовать рассмотрение полей именно как полей гомоморфизмов.

Приведенные соображения очень абстрактные. Как на самом деле найти числовые поля, которые являются полями Галуа над **Q**? Ответ будет простой. Возьмем любой многочлен с рациональными коэффициентами $f(X) \in \mathbf{Q}[X]$. Разложим $f(X)$ на множители над комплексными числами

$$f(X) = a(X - \alpha_1)(X - \alpha_2) \cdot \cdot \cdot (X - \alpha_n)$$

и пусть $K = \mathbf{Q}(\alpha_1, \alpha_2, \ldots, \alpha_n)$ будет наименьшим подполем **C**, что содержит все α_i. Тогда любой гомоморфизм $\sigma: K \to \mathbf{C}$ определяется значениями $\sigma(\alpha_1)$, . . . , $\sigma(\alpha_n)$, и каждое $\sigma(\alpha_i)$ должно быть корнем $f(X)$ и, значит, должно равняться некоторому α_j. Тогда, $\sigma(\alpha_i) \in K$, так что $\sigma(K) \in K$ (включение $\sigma(K) \subset K$ является очевидным, и тогда равенство следует из сравнения степеней расширений $\sigma(K)$ и *K* над **Q**). Поле K, очевидно, является *полем разложения* f(X) *над* **Q**, и если многочлен f(X) не имеет кратных корней ($\alpha_i \neq \alpha_j$), то можно убедиться в том, что такое поле является расширением Галуа. И наоборот, можно доказать, что если числовое поле *K* является расшире-

[13] Группа Галуа – группа автоморфизмов Галуа расширения *L* поля *k*, т.е. группа, которая состоит из всех автоморфизмов поля *L*, которые оставляют все элементы подполя *k* неподвижными. Группа Галуа обозначается G(L/k).

нием Галуа поля **Q**, то оно является полем разложения некоторого многочлена $f(X) \in \mathbf{Q}[X]$.

Возвратимся теперь к эллиптическим кривым. Как уже отмечалось ранее, в криптографических приложениях эллиптическая кривая рассматривается над некоторым конечным полем K (полем Галуа $GF(p^n)$), т.е. кривая $E(K)$ над полем K определяется как множество точек $(x, y) \in K \times K$, которые являются решениями уравнения (1), где a, b, c $\in$ K являются константами, вместе с дополнительной точкой O – ″точкой на бесконечности″. Соответственно условию 1 относительно отбора эллиптических кривых, рассмотренному выше, константы a, b, c должны быть выбранными таким образом, чтобы кривая C была несингулярной.

Нас будет интересовать точки эллиптической кривой порядка n, которые образуют группу кручения C[n] (подгруппу группы комплексных точек кривой *C*), т.е.

$$E[n] := \left\{ P \in E(\overline{K}) : \ nP = 0 \right\}$$

(напомним, что $\overline{K}$ обозначает замыкание поля *K*, см. [4, 5]).

Будем рассматривать C[n] как абстрактную группу. Справедливо такое утверждение [3].

Утверждение. *Как абстрактная группа* C[n] *является прямой суммой двух циклических групп порядка n, т.е.*

$$C[n] \cong \frac{\mathbf{Z}}{n\mathbf{Z}} \oplus \frac{\mathbf{Z}}{n\mathbf{Z}}.$$

Это утверждение, как видим является частным видом представления (3), и оно означает, что C[n] порождается двумя ″базисными″ элементами, скажем, P_1 и P_2. Следовательно, соответственно выражению (4) элементы C[n] могут быть представлены в виде множества

$$\left\{ a_1 P_1 + a_2 P_2 : a_1, a_2 \in \frac{\mathbf{Z}}{n\mathbf{Z}} \right\},$$

и, значит, каждый элемент C[n] может быть записан для *уникальной* пары элементов $a_1, \ a_2 \in \mathbf{Z} / n\mathbf{Z}$ как $a_1 P_1 + a_2 P_2$.

Снова следуя [3], рассмотрим теперь более подробно так называемый *мультипликативный n-гомоморфизм*

$$\varphi: \ C(\mathbf{C}) \xrightarrow[\text{на n}]{\text{умножение}} C(\mathbf{C}), \ \ P \mapsto nP.$$

Очевидно, что ядром гомоморфизма $\varphi(P) = nP$ является именно подгруппа C[n], т.е.

$$C[n] = \mathrm{Ker}(\varphi) = \left\{ P \in C(\mathbf{C}) : nP = O \right\}.$$

Так как P имеет порядок, который равняется точно n, то это будет множество точек, порядки которых делятся на n.

Подчеркнем, и это принципиально, что мультипликативный *n-гомоморфизм* на C(**C**) имеет специфическое свойство, а именно – это отображение определяется при помощи рациональных функций, т.е. x, y координаты точки n являются рациональными функциями x, y координат точки P.

Например, если P = (x, y) является точкой на эллиптической кривой

$$y^2 = x^3 + ax^2 + bx + c,$$

это после выполнения вычислений можно обнаружить, что

$$2P = \left(\frac{g(x)}{4y^2}, \frac{h(x)}{8y^2} \right),$$

где $g(x) = x^4 - 2bx^2 - 8cx + b^2 - 4ac$;

$$h(x) = x^6 + 2ax^5 + 5bx^4 + 20cx^3 + 5(4ac - b^2)x^2 + $$
$$+2(4a^2c - ab^2 - 2bc)x + 4abc - b^3 - 8c^2.$$

В общем случае гомоморфизм, который определяется по помощи рациональных функций, называется *изогенией*.

Таким образом, изогения является гомоморфизмом $\varphi : C(\mathbf{C}) \to C(\mathbf{C})$, который имеет форму

$$\varphi(x, y) = \left(\frac{\text{многочлен от x и y}}{\text{многочлен от x и y}}, \frac{\text{многочлен от x и y}}{\text{многочлен от x и y}} \right).$$

Криптографические преобразования выполняются на основе именно отображения (5), т.е. исходные точки эллиптической кривой превращаются в точки этой же группы. Поэтому нас должны интересовать изогении эллиптических кривых в себя. Такие изогении называются *эндоморфизмами*[14] (или иногда *алгебраическими эндоморфизмами*, чтобы подчеркнуть тот факт, что они определяются через рациональные функции). Каждая эллиптическая кривая имеет мультипликативный *n*-эндоморфизм (5), один для каждого целого *n*. Анализ показывает, что большинство эллиптических кривых не имеет других эндоморфизмов. Однако, есть некоторые эллиптические кривые с дополнительными эндоморфизмами, которые не являются мультипликативными *n*-эндоморфизмами. Мы сфокусируем наше внимание именно на этих особых эллиптических кривых, которые, как мы увидим дальше, заслуживают того, чтобы дать им специальное имя.

Определение. *Пусть* C *будет эллиптической кривой. Мы будем говорить, что* C *имеет комплексное умножение, если существует эндоморфизм* $\varphi : C \to C$, *который не является мультипликативным n-отображением.* (5)

Будет полезным сразу же привести примеры заимствованные из [3] эллиптических кривых, которые имеют комплексное умножение.

[14] Под эндоморфизмом алгебраической системы *A* понимается отображение алгебраической системы в себя, которое согласовано с ее структурой. В данном случае изогения и определяет согласованность гомоморфизма, который она определяет с помощью рациональной функции, со структурой группы точек эллиптической кривой. Понятие эндоморфизма является частным случаем понятия гомоморфизма двух алгебраических систем.

П р и м е р 1. Эллиптическая кривая

$$C : y^2 = x^3 + x$$

имеет комплексное умножение

$$\varphi(x, y) = (-x, iy),$$

так как, если $y^2 = x^3 + x$, то

$$(iy)^2 = -y^2 = -x^3 - x = (-x)^3 + (-x)$$

(рдесь $i = \sqrt{-1}$, по обыкновению).

П р и м е р 2. Эллиптическая кривая

$$C : y^2 = x^3 + 1$$

имеет комплексное умножение

$$\varphi(x, y) = \left(\left(\left(-1 + \sqrt{-3}\right)/2\right)x, -y\right),$$

так как $\left(\left(-1 + \sqrt{-3}\right)/2\right)^3 = 1$, и легко увидеть, что $\varphi(x, y)$ действительно является точкой на *C*.

В более общем случае, если φ_1 и φ_2 являются эндоморфизмами кривой *C*, то мы можем определить новый эндоморфизм $\phi_1 + \phi_2$ так

$$(\varphi_1 + \varphi_2) : C \to C, \ (\phi_1 + \varphi_2)(P) = \varphi_1(P) + \varphi_2(P).$$

Мы также получим новый эндоморфизм, если возьмем композицию

$$(\varphi_1 \cdot \varphi_2) : C \to C, (\phi_1 \cdot \varphi_2)(P) = \varphi_1(\varphi_2(P)).$$

С этим ″сложением″ и ″умножением″ множество эндоморфизмов кривой *C* становится кольцом $\mathrm{End}(E)$. Если эллиптическая кривая *C* не имеет комплексного умножения, то это кольцо обязательно изоморфно **Z**, т.е. обычному кольцу целых чисел (*в таком кольце существуют только эндоморфизмы* $\varphi : C \to C$*, которые являются мультипликативными n-отображениями*). Особенностью кольца эндоморфизмов в этом случае является его некоммутативность.

Эндоморфизм $\phi : C \to C$ дает гомоморфизм

$$\phi : C[n] \to C[n]$$

(так, если $P \in C[n]$, то $n\phi(P) = \phi(nP) = \phi(O) = O$ и, итак, $\phi(P) \in C[n]$). Это означает, что существуют элементы a, b, c, d $\in \in$ **Z/n** такие, что $\phi(P_1) = a_1 + c_2$, $\phi(P_2) = b_1 + d_2$, т.е. гомоморфизму $\phi : C[n] \to C[n]$ соответствует матрица $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Кольцо таких матриц не коммутативное, например, матрицы $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ и $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ не коммутативны.

И именно в этом случае можно применить спаривание Вейля, которое мы рассматривали на предыдущей лекции.

Но, если C имеет комплексное умножение, то кольцо эндоморфизмов является точно более широким, чем **Z**.

Рассмотрим этот случай более подробно.

Пусть $K / \mathbf{Q}$ будет любым Галуа расширением с мнимой единицей $i \in K$, и пусть $\sigma \in \mathrm{Gal}(K / \mathbf{Q})$. Тогда для любой точки $P \in C(K)$ эллиптической кривой с комплексным умножением мы имеем два пути, чтобы получить новую точку в $C(K)$, а именно мы можем применить эндоморфизм φ к *P*, или мы можем применить элемент расширения Галуа σ к *P*. Мы спросим, где σ и φ коммутативные? Другими словами, когда верно, что

$\sigma(\varphi(P)) = \varphi(\sigma(P))$ для каждой точки $P \in C(K)$?

Используя введенные высшее определение и пример, мы можем увидеть, что для $\varphi(P) = \varphi(x, y) = (-x, iy)$

$$\sigma(\varphi(P)) = \sigma(-x, iy) = (\sigma(-x), \ \sigma(iy)) = (-\sigma(x), \ \sigma(i)\sigma(y));$$

$$\varphi(\sigma(P)) = \varphi(\sigma(x), \sigma(y)) = (-\sigma(x), \ i\,\sigma(y)).$$

Итак, σ и φ коммутативны при условии, что $\sigma(i) = i$: другими словами, они будут коммутативные, если $\sigma \in \mathrm{Gal}(K / \mathbf{Q}(i))$. Поэтому, если мы идем к рассмотрению отображения φ, чтобы использовать группы Галуа, то мы это будем это делать в смысле рассмотрения Галуа расширений $\mathbf{Q}(i)$ скорее чем **Q**. Именно эллиптические кривые с коммутативным эндоморфизмом $\mathrm{End}(C)$ и являются теми, которые нужны для криптографических применений.

Особенностью этих кривых является то, что порядок базовых точек для таких кривых удовлетворяет отмеченному выше ограничению ($2^{ml} \neq 1 (\mathrm{mod}\, n)$, для $1 \le l \le 32$). Эти кривые были названы *несуперсингулярными* в отличие от *суперсингулярных* эллиптических кривых, в которых кольцо эндоморфизмов некоммутативно. Зафиксируем этот факт в форме определения.

Определение. *Эллиптическая кривая называется суперсингулярной, если кольцо эндоморфизмов* $\mathrm{End}(C)$ *некоммутативное*.

В заключение заметим также, что вместе с определением несуперсингулярности через свойства колец эндоморфизмов используются также и другие (эквивалентные) определение. Например, для ″суперсингулярности″ кривой *E*, которая задана уравнением

$$E : \ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

можно воспользоваться выполнением любого из следующих условий: (i) $a_1 = 0$, (*ii*) $|E(K)|$ является четным ($K = F(p^m)$), (*iii*) *j-инвариант E* является нулем (для полей характеристики два). Обоснование этих условий выходит за рамки настоящей работы.

Непригодными для криптографических применений считаются также так называемые *аномальные кривые*. Эллиптическая кривая *E,* определенная над $F(p)$, называется аномальной, если #(E) = p (p – про-

стое число), т.е. это такая кривая, группа точек которой совпадает с обычной группой простого порядка.

В качестве общего вывода этого раздела можно отметить, что именно несуперсингулярные эллиптические кривые при построении криптосистем открывают возможность широкого выбора между многими разными группами разного порядка. Эта различие оказывается дополнительным их преимуществом по сравнению с использованием групп конечных полей, где имеется только один кандидат для каждого поля. В то же время, существование изоморфного отображения для некоторого множества точек эллиптической кривой $E(K) = E\left(F_q\right)$ на подгруппу мультипликативной группы расширения поля F_q позволяет свести задачу дискретного логарифмирования для суперсингулярной эллиптической кривой к нахождению дискретного логарифма в конечном поле Галуа (для суперсингулярной кривой можно построить расширение поля с небольшой степенью расширения 1).

Заключение

В заключение отметим, что дальнейшие исследования в теории эллиптических кривых позволили найти полезное применение в криптографии и для суперсингулярных эллиптических кривых. В работах [12, 13] признанные специалисты криптографы Sakai, Ohgishi и Kasahara и Joux независимо друг от друга предложили применить процедуры билинейных спариваний точек эллиптических кривых в разработанных ими новых криптографических системах и протоколах. Их предложения позволяют поновому подойти к эффективной реализации криптографических протоколов установления, согласования и подтверждения ключей, разделения секрета и других механизмов управления ключами. Разрешение многих из существующих здесь противоречий специалисты видят в применении методов открытой криптографии, которая базируется на идентификаторах пользователей совместно с билинейными преобразованиями на основе спаривания точек сингулярных и иных эллиптических кривых [14]. Это интересное направление заслуживает отдельного детального обсуждения.

Список литературы

1. Miller V.C. Use og Elliptic Curve in Cryptography // Cryptology: Proceedings of Crypto 85, Springer LNCS 218, 1986. – P. 417-426.

2. Lenstra H.W. Factoring integers with elliptic curves // Ann. Of Vath, (2) 126 (1987). – H. 674-745.

3. Silverman J. The Arithmetic of Elliptic Curves. – New York: Springer-Verlag, 1986.

4. Долгов В.И., Лисицкая И.В. Теория групп и колец: Конспект лекцій з дисципліни "Спеціальні розділи математики". – Х.: ХТУРЭ, 2000.

5. Завало С.Т. и др. Алгебра и теория чисел. – К.: Вища шк., 1980. – Ч.2. – 402 с.

6. Beth Y., Schaefer F. Non Supersingular Elliptic Curves for Public Key Cryptosystems. – Copyring © 1998, Springer-Verlag.

7. Diffie W., Hellman M. E. New Directions in Cryptography // IEEE Transactions on Information Theory. – November 1976. – V.IT-22, n.6. – P. 644-654.

8. Koblitz N. Eliptic Curve Cryptosystems // Mathematics of Computation. – 1987. – V. 48, № 177. – P. 203-209.

9. Menezes A., Okamoto T., Vanstone S. Reducing Elliptic Curve Logarithms to a Finite Field // IEEE Trans. Info. Theory. – 1993. – 39. – P. 1603-1646.

10. Coppersmith D. Fast evaluation of logarithms in fields of characteristic two // IEEE Trans. Inform. Theory. – 1984. – IT 30. –P. 587-594.

11. Koblitz N. Constructing Elliptic Curve Cryptosystems in Characteristic 2. – Springer-Verlag, 1998.

12. Joux A. A one round protocol for tripartite Diffie-Hellman // W. Bosma, editor, Algorithmic Number Theory, IV-th Symposium (ANTS IV), Lecture Notes in Computer Science 1838. – Springer-Verlag, 2000. – P. 385-394.

13. Sakai R., Ohgishi K., Kasahara M. Cryptosystems based on pairing // Proceedings of the 2000 Symposium on Cryptography and Information Security, Okinawa, Japan, January 2000.

14. Blake, G. Seroussi, Smart N. Elliptic Curves in Cryptography. Cambridge University Press, 1999. London Mathematical Society Lecture Note Series 265.

Поступила в редколлегию 22.09.2008

Рецензент: д-р техн. наук, проф. Ю.В. Стасев, Харьковский университет Воздушных Сил им. И. Кожедуба, Харьков.

ЕЛІПТИЧНІ КРИВІ В КРИПТОГРАФІЇ

В.І. Долгов

Визначаються умови, які повинні бути враховані при відборі еліптичних кривих для криптографічних застосувань. Приводиться відповідний понятійний апарат, зокрема визначаються поняття сингулярності і суперсингулярності для еліптичних кривих і розглядаються теоретичні положення, лежачі в їх основі.

Ключові слова: *криптографія, еліптична крива, сингулярність, суперсингулярність.*

ELLIPTIC CURVES ARE IN CRYPTOGRAPHY

V.I. Dolgov

Terms which must be taken into account at the selection of elliptic curves for cryptographic applications are determined. The proper concept vehicle over is brought, in particular the concepts of singularity and supersingularity are determined for elliptic curves and theoretical positions, lyings in their basis, are examined.

Keywords: *cryptography, elliptic curve, singularity, supersingularity.*